



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,319	07/02/2001	G. Scott Smith	020699-000310US	4767

37490 7590 05/04/2005

CARPENTER & KULAS, LLP  
1900 EMBARCADERO ROAD  
SUITE 109  
PALO ALTO, CA 94303

EXAMINER

GELAGAY, SHEWAYE

ART UNIT PAPER NUMBER

2133

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/898,319

Applicant(s)

SMITH ET AL.

Examiner

Shewaye Gelagay

Art Unit

2133

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 17 December 2004.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-15 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### **Response to Arguments**

1. This office action is in response to Applicant's amendment filed on December 17, 2004. Claims 1-5 have been amended, claims 8-15 are added. Claims 1-15 are pending.

Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection. Applicant's arguments, see Remarks, filed December 17, 2004, with respect to the rejection(s) of claim(s) 1 have been considered but are not persuasive.

Applicant argues Cane stores its key and data in two separate storage device, however, a single storage media is added in the amendment and a new ground of rejection is necessitated.

Applicant argues Cane does not teach combining the encrypted content with the second key. Examiner disagrees with the Applicant because Cane teaches associating the encrypted key with the encrypted file (Col. 4 lines 20-22). Associating of the encrypted key with the encrypted file has the same functionality as combining because they both create the connection between the encryption key and the encrypted data.

Applicant requested the accurately translated copy of Oomori (including Figure legends) into English be provided. However, Examiner did not use Oomori in any of the communication sent to the Applicant.

***Claim Objections***

2. Claim 6 is objected to because of the following informalities: The word "retrieving" is changed to "receiving", however, the claim status has not been changed from original to currently amended. Appropriate correction is required.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Art Unit: 2133

4. Claims 1-4, 6-7, 10-11 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cane et al. (hereinafter Cane) United States Letters Patent Number 5,940,507 in view of Noda et al. (hereinafter Noda) United States Letters Patent Number 6,671,759 and in view of Deindl et al. (hereinafter Deindl) United States Letters Patent Number 6,031,910.

As per claims 1 and 10:

Cane teaches a communication system having a terminal for receiving encrypted content, the terminal being coupled to a single storage media via an IEEE 1394 serial bus, a method for storing the encrypted content on the storage media the method and apparatus comprising:

encrypting a first key for decrypting the encrypted content to form a second key; (Col. 3, lines 59-60; The master encryption key is obtained and used to encrypt the secondary key and produce an encrypted key)

combining the encrypted content with the second key to form a combined encrypted content; (Col. 4 lines 20-22; the encrypted key is then written to a tape index disk file thereby associating the magnetic tape volume with the encrypted file and the encrypted key) and

Cane does not explicitly disclose receiving the encrypted content via the IEEE 1394 bus; and storing the combined encrypted content on the single storage media.

Noda et al. in analogous art, however, disclose receiving the encrypted content via the IEEE 1394 bus. (Col. 14; lines 6-8; the encrypted data is received by the IEEE 1394 Interface of the optical disk drive through the IEEE 1394 bus)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Cane to include a step of receiving the encrypted content via the IEEE 1394 bus. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the suggestions, provided by Noda et al. (Col. 1; lines 18-19) in order to have high transmission speed and mutual communications between electronic devices.

Both references do not explicitly disclose storing the combined encrypted content on the single storage media.

Deindl in analogous art, however, discloses storing the combined encrypted content on the single storage media. (Col. 2, lines 33-34; Col. 6, lines 31-32)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method and apparatus disclosed by Cane and Noda to include storing the combined encrypted content on the single storage media. This modification would have been obvious because a person having ordinary skill in the art would have been motivated as suggested by Deindl (Col. 1, lines 7-8) for securing the transmission and storage of protectable information.

As per claim 2:

Cane, Noda and Deindl teach all the subject matter as discussed above. In addition, Cane further discloses a method comprising:

Art Unit: 2133

retrieving the combined encrypted content from the storage media; (Col. 4; lines 27-28; recovery of a file is accomplished by the archive server referencing the index to obtain the encrypted key and the volume of the encrypted file. The encrypted file is then retrieved from the volume)

decrypting the second key to obtain the first key; (Col. 4; lines 24-35; the secondary key must be recovered by decrypting the encrypted key with the master key.) and

decrypting the encrypted content with the first key to recover clear text content. (Col. 4; lines 35-36; the original file may be recovered by decrypting the encrypted file with the secondary key.)

In addition, Deindl further discloses the use of a single storage media. (Col. 2, lines 33-34; Col. 6, lines 31-32)

As per claims 3 and 13:

Cane, Noda and Deindl teach all the subject matter as discussed above. In addition, Cane further discloses a method and an apparatus comprising:

further encrypting the second key prior to storage on the single media. (Col. 3, lines 59-60; Col. 4 lines 20-22)

As per claims 4 and 11:

Cane, Noda and Deindl teach all the subject matter as discussed above. In addition, Cane further discloses a method and an apparatus wherein the combined encrypted content includes a stream. (Col. 4 lines 20-22)

As per claim 6:

Cane, Noda and Deindl teach all the subject matter as discussed above. In addition, Cane further discloses a method comprising:

receiving the second key and the encrypted data; (Col. 4; lines 27-28)  
decrypting the second key to form the first key; (Col. 4; lines 24-35) and  
decrypting the encrypted data with the first key to form clear text. (Col. 4; lines 35-36)

As per claim 7:

Cane, Noda and Deindl teach all the subject matter as discussed above. In addition, Cane further discloses a method comprising: decrypting the encrypted content with the first key to recover clear text content. (Col. 4; lines 35-36) and forwarding the combined encrypted data (Col. 3, lines 65-66). Not explicitly disclosed by Cane is that "encrypting the clear text using a third key to form combined encrypted data." However, Cane further teach the master key is used to encrypt multiple keys that will be used in encrypting successive files. (Col. 3; lines 62-63; the same master key is used to encrypt multiple secondary keys it needs to be generated once and then reused for successive secondary keys.) This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated in order to have extra security. To maintain security and integrity of stored data by maintaining a series of keys for each archived file. (Col. 2; lines 38-39)

5. Claims 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cane et al. (hereinafter Cane) United States Letters Patent Number 5,940,507 in view



of Noda et al. (hereinafter Noda) United States Letters Patent Number 6,671,759 in view of Deindl et al. (hereinafter Deindl) United States Letters Patent Number 6,031,910 and further in view of Nozawa et al. (hereinafter Nozawa) United States Letters Patent Number 5,235,641.

As per claims 5 and 12:

Cane, Noda and Deindl teach all the subject matter as discussed above. Neither of the references explicitly disclose including a header in the combined encrypted content.

Nozawa in analogous art, however, discloses including a header in the combined encrypted content. (Col. 5; lines 47-48; write the encrypted data key into a header portion or the like at the beginning of an ordinary data recording area)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method and apparatus disclosed by Cane, Noda and Deindl to include a header in the combined encrypted content. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the suggestions, provided by Nozawa (Col. 6; lines 36-45) to retrieve the encrypted data easily by reading the header portion first.

6. Claims 8-9 and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cane et al. (hereinafter Cane) United States Letters Patent Number 5,940,507 in view of Noda et al. (hereinafter Noda) United States Letters Patent Number 6,671,759

Art Unit: 2133

and in view of Deindl et al. (hereinafter Deindl) United States Letters Patent Number 6,031,910 and further in view of Just et al. (hereinafter Just) United States Letters Patent Number 6,567,914.

As per claims 8 and 14:

Cane, Noda and Deindl teach all the subject matter as discussed above. Neither of the references explicitly disclose a method wherein the further encrypting uses a different algorithm than that used that used in encrypting the first key.

Just in analogous art, however, discloses a method and apparatus wherein the further encrypting uses a different algorithm than that used that used in encrypting the first key. (Col. 8; lines 9-14)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method and apparatus disclosed by Cane, Nodaand Deindl to include wherein the further encrypting uses a different algorithm than that used that used in encrypting the first key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the suggestions, provided by Just (Col. 8; lines 15-16) in order to facilitate a higher level of security for the encrypted message.

As per claims 9 and 15:

Cane, Noda, Deindl and Just teach all the subject matter as discussed above. In addition, Just further discloses a method and apparatus wherein an algorithm includes one or more of DES, XOR, M2, M6+, IDEA. (Col. 7, lines 13-18)

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.
8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

4/29/2005

Shewaye Gelagay   
Examiner  
Art Unit 2133



**GUY LAMARRE**  
**PRIMARY EXAMINER**